IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Civil Action No. 1:15-cv-00662-TSE

Attachment

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

ORDER GRANTING DEFENDANTS' MOTION FOR SUMMARY JUDGMENT AND DENYING PLAINTIFFS' CROSS-MOTION

_____/

Now before the Court is the motion for summary judgment filed by Defendants National Security Agency, United States, Department of Justice, Paul M. Nakasone, Donald J. Trump, William Barr, and Daniel Coats, in their official capacities (collectively, "Defendants") and the cross-motion to proceed to resolution on the merits filed by Plaintiffs Carolyn Jewel, Tash Hapting, Young Boon Hicks, as executrix of the estate of Gregory Hicks, Erik Knutzen, and Joice Walton, on behalf of themselves and all other individuals similarly situated ("Plaintiffs").

Having considered the parties' papers, including Defendants' classified submissions, and the parties' arguments, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion for summary judgment.

BACKGROUND

A. Factual Procedural Background.

This case is one of many arising from claims that the federal government, with the assistance of major telecommunications companies, conducted widespread warrantless dragnet communications surveillance of United States citizens following the attacks of September 11, 2001. On September 18, 2008, Plaintiffs filed this putative class action on behalf of themselves and a class of similarly situated persons described as "millions of ordinary Americans . . . who use[] the phone system or the Internet" and "a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant or court order since September 12, 2001." (Complaint at ¶¶ 1, 7, and 9.) The Court is now faced with the challenge of determining whether, as Plaintiffs describe it, the data and metadata collection programs may violate Plaintiffs' remaining statutory protections afforded them by the Wiretap Act and the Electronic Communications Privacy Act or the Stored Communications Act. Further, the Court is tasked with the preliminary question whether the Plaintiffs may maintain their claims based on the evidence of their standing and the potential that continued litigation may imperil national security.

According to the allegations in the Complaint, a program of dragnet surveillance (the "Program") was first authorized by Executive Order of the President on October 4, 2001. (*Id.* at ¶¶ 3, 39.) Under this Program (and subsequently under statutory authorities) the NSA undertook the collection of non-content telephony and Internet metadata in bulk, and the contents of certain Internet communications. (*See id.* at ¶¶ 3-13, 39; *see also* Dkt. No. 389, Declaration of Michael S. Rogers ("Rogers Decl.") ¶¶ 40, 47-48, 51-52.) Plaintiffs allege that, in addition to eavesdropping on or reading specific communications, Defendants have "indiscriminately intercepted the communications content and obtained the communications records of millions of ordinary Americans as part of the Program authorized by the President." (Complaint ¶ 7.) The core component of the Program is a nationwide network of sophisticated communications surveillance devices attached to the key facilities of various

telecommunications companies that carry Americans' Internet and telephone communications. (*Id.* at ¶¶ 8, 42.) Plaintiffs allege that Defendants have unlawfully solicited and obtained the private telephone and internal transactional records of millions of customers of the telecommunications companies, including records indicating who the customers communicated with, when those communications took place and for how long, among other sensitive information. Plaintiffs allege these records include both domestic and international communications. (*Id.* at ¶ 10.) Plaintiffs sue Defendants "to enjoin their unlawful acquisition of the communications and records of Plaintiffs and class members, to require the inventory and destruction of those that have already been seized, and to obtain appropriate statutory, actual, and punitive damages to deter future illegal surveillance." (*Id.* at ¶ 14.)

Plaintiffs originally alleged seventeen counts against Defendants: violation of the Fourth Amendment (counts 1 and 2); violation of the First Amendment (counts 3 and 4); violation of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1809, 1810 (counts 5 and 6); violation of the Wiretap Act, 18 U.S.C. § 2511(1)(a), (b), and (d) (counts 7 through 9); violation of the Electronic Communications Privacy Act or the Stored Communications Act, 18 U.S.C. § 2703(a), (b), and (c) (counts 10 through 15); violation of the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.* (count 16); and violation of separation of powers (count 17).

After the Complaint was filed on September 18, 2008, Defendants moved to dismiss and alternatively sought summary judgment as to all claims. Defendants argued that the Court lacked jurisdiction over the statutory claims because the Government had not waived its sovereign immunity. Defendants moved for summary judgment on the remaining claims based primarily on the contention that the information necessary to litigate the claims was properly subject to the state secrets privilege.

The district court, the Honorable Vaughn R. Walker presiding, dismissed the claims without leave to amend based on the finding that Plaintiffs had failed to make out the *prima facie* allegations necessary to establish standing. (Dkt. No. 57.)

On appeal, the Ninth Circuit Court of Appeals reversed the district court's dismissal of the Complaint on the ground of lack of standing. The appeals court concluded that, at the pleadings stage, "Jewel [had] alleged a sufficiently concrete and particularized injury. Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches." *See Jewel v. National Security Agency*, 673 F.3d 902, 909-10 (9th Cir. 2011). Although the appellate court remanded on the basis that it was premature to dismiss premised upon lack of standing, the court noted that "procedural, evidentiary, and substantive barriers" might ultimately doom Plaintiffs' proof of standing. *See id.* at 911. The court remanded "with instructions to consider, among other claims and defenses, whether the government's assertion that the state secrets privilege bars this litigation." *Id.* at 913-14.

Upon remand, Plaintiffs filed a motion for partial summary adjudication urging the Court to reject Defendants' state secret defense. Defendants cross-moved to dismiss on the basis of sovereign immunity for the statutory claims and for summary judgment on the assertion of the state secrets privilege.

On July 23, 2013, this Court granted Plaintiffs' motion for partial summary adjudication by rejecting the state secrets defense as having been displaced by the statutory procedure prescribed in 50 U.S.C. Section 1806(f) of FISA. (Dkt. No. 153.) The Court granted Defendants' motions to dismiss Plaintiffs' claims for damages under FISA and all statutory claims for injunctive relief on the basis of sovereign immunity. Further, the Court reserved ruling on the Defendants' motions for summary judgment on the remaining non-statutory claims.

On July 25, 2014, Plaintiffs moved for partial summary judgment on their Fourth Amendment claims and on September 29, 2014, Defendants cross-moved on the threshold issue of standing and on the merits of the Fourth Amendment claim. On February 10, 2015, this Court denied Plaintiffs' motion and granted Defendants' motion for partial summary judgment on Plaintiffs' Fourth Amendment claims. (Dkt. No. 321.) Relying on both the public record and Defendants' classified submissions, the Court found that Plaintiffs had failed to establish a sufficient factual basis to assert they had standing to sue under the Fourth Amendment

regarding the possible interception of their Internet communications. Further, the Court found that the Fourth Amendment claim would otherwise have to be dismissed because even if Plaintiffs could establish standing, such a potential claim would have to be dismissed on the basis that any possible defenses would require the impermissible disclosure of state secret information.

On May 20, 2015, this Court granted Defendants' motion for entry of judgment under Federal Rule of Civil Procedure 54(b) on the basis that the threshold issue of standing and its adjudication in the Fourth Amendment context was a final determination and no just reason existed for delay in entering final judgment on the constitutional claim. (Dkt. No. 327.)

Plaintiffs appealed that ruling, and on December 18, 2015, the Ninth Circuit, dismissed the appeal, reversed the certification, and remanded to this Court. (Dkt. No. 333.) The appellate court found that the severable claim of liability under the Fourth Amendment did not encompass all plaintiffs or defendants or all remaining claims and therefore the piecemeal resolution of individual issues did not satisfy the requirements of Rule 54(b). The Ninth Circuit remanded with instructions to expend the parties' and the district court's resources in an effort to obtain a final and comprehensive judgment of this entire matter.

Immediately upon remand, on February 19, 2016, this Court lifted the stay of discovery on the remaining statutory claims and admonished the parties to seek resolution of all remaining matters by summary adjudication on the merits, with the benefit of any potentially available discovery. (Dkt. No. 340.) The Court permitted Plaintiffs to serve discovery requests limited to the issue of their standing to pursue the remaining statutory claims. The Court directed Defendants to file its unclassified objections and responses to Plaintiffs' requests in the public record, and to submit classified documents and information responsive to Plaintiffs' discovery requests *ex parte* and *in camera*. The Court also tasked the Defendants to marshal all evidence bearing on the issue of Plaintiffs' standing, even if it had not been specifically requested by Plaintiffs. (Dkt. No. 356.)

On August 17, 2018, after having reviewed both the classified and public materials produced and in the record, this Court issued an order requiring the parties to file cross motions

for summary judgment on the issue of Plaintiffs' standing or lack of standing as to each of the remaining claims. (Dkt. No. 410.)

The currently pending cross-motions are now ripe for resolution.

B. Legal Framework Background.

In its order dated July 23, 2013, the Court found that, after the Ninth Circuit remanded this Court's order finding that Plaintiffs lacked standing prior to the proffer of discovery, the Court could utilize the statutory procedure prescribed in 50 U.S.C. Section 1806(f) of FISA ("Section 1806(f)") in order to address the ongoing litigation. Further, the Court found that the state secrets defense did not require immediate dismissal of the matter. In that order, the Court found that the use of the procedural mechanism established by Section 1806(f) would not automatically result in the summary exclusion of all potentially classified information. Rather than merely permitting the assertion of the state secrets privilege to result in immediate dismissal of this action, the Court has, on numerous occasions, permitted Defendants to supply classified evidence for the Court's *in camera* review. *See also In re National Security Agency Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1111 (N.D. Cal. 2008) ("FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes . . . ."). Having found that Section 1806(f) of FISA displaces the state secrets privilege as a procedural mechanism in cases in which electronic surveillance yields potentially sensitive evidence by providing secure procedures under which courts can consider national security evidence, this Court has determined that the application of the state secrets privilege would not automatically apply to summarily exclude litigation of this action.

Subsequent to this Court's determination that FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes, the Ninth Circuit similarly and more recently concluded that "in enacting FISA, Congress displaced the common law dismissal remedy created by the *Reynolds* state secrets privilege as applied to electronic surveillance within FISA's purview." *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1230 (9th Cir. 2019). The court held that the electronic surveillance claims brought by the plaintiffs in that case were "not subject to outright dismissal at the pleading stage," and

remanded so that the district court could employ the procedures established by Section 1806(f) to review evidence over which Defendants had asserted the state secrets privilege. *Id.* at 1226, 1251. This Court has, in the lengthy course of this case, employed those procedures.

Now, having required briefing on the remaining statutory claims and having required the proffer of evidence regarding standing from both Plaintiffs and Defendants, both public and classified, the Court may determine the full extent of the threshold legal issue regarding whether Plaintiffs have standing to sue and the determination, regardless whether Plaintiffs have standing to sue, if the Court may proceed to the merits of this case. As discussed at greater length in Section II of the Court's Supplemental Classified Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiffs' Cross-Motion ("Classified Order") filed herewith, after over ten years of litigation and multiple disclosures, the Court accepts the representation of the Defendants that they are unable to defend the litigation or to pursue it to resolution on the merits without grave risk to the national security.

ANALYSIS

A. Legal Standard on Motion for Summary Judgment.

A principal purpose of the summary judgment procedure is to identify and dispose of factually unsupported claims. *Celotex Corp. v. Cattrett*, 477 U.S. 317, 323-24 (1986). Summary judgment is proper when the "pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). "In considering a motion for summary judgment, the court may not weigh the evidence or make credibility determinations, and is required to draw all inferences in a light most favorable to the non-moving party." *Freeman v. Arpaio*, 125 F.3d 732, 735 (9th Cir. 1997).

The party moving for summary judgment bears the initial burden of identifying those portions of the pleadings, discovery, and affidavits that demonstrate the absence of a genuine issue of material fact. *Celotex*, 477 U.S. at 323; *see also* Fed. R. Civ. P. 56(c). An issue of fact is "genuine" only if there is sufficient evidence for a reasonable fact finder to find for the non-

moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). A fact is "material" if it may affect the outcome of the case. *Id.* at 248. Once the moving party meets its initial burden, the non-moving party must go beyond the pleadings and, by its own evidence, "set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e).

In order to make this showing, the non-moving party must "identify with reasonable particularity the evidence that precludes summary judgment." *Keenan v. Allan*, 91 F.3d 1275, 1279 (9th Cir. 1996) (quoting *Richards v. Combined Ins. Co.*, 55 F.3d 247, 251 (7th Cir. 1995) (stating that it is not a district court's task to "scour the record in search of a genuine issue of triable fact"); *see also* Fed. R. Civ. P. 56(e). If the non-moving party fails to point to evidence precluding summary judgment, the moving party is entitled to judgment as a matter of law. *Celotex*, 477 U.S. at 323; *see also* Fed. R. Civ. P. 56(e)(3).

B. Legal Standard on Threshold Issue of Standing.

"[T]here can be no genuine issue as to any material fact" where a party "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which [it bears] . . . the burden of proof." *Celotex*, 477 U.S. at 322. Standing is "an essential . . . part of the case-or-controversy requirement of Article III." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). In order for Plaintiffs to establish Article III standing, they must show they: "(1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the [Defendants], (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, __ U.S. __, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan*, 504 U.S. at 650-61). Plaintiffs bear the burden of proving the existence of standing to sue. *See, e.g., United States v. Hays*, 515 U.S. 737, 743 (1995). Plaintiffs must be able to establish standing for each claim and for each form of relief. *See, e.g., DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006); *Davidson v. Kimberly Clark*, 889 F.3d 956, 967 (9th Cir. 2018).

"In other words, plaintiffs here must show *their own* metadata was collected by the government." *Obama v. Klayman*, 800 F.3d 559, 562 (D.C. Cir. 2015) (citations omitted; emphasis in original); *see also Halkin v. Helms*, 690 F.2d 977, 999-1000 (D.C. Cir. 1982) ("[T]he absence of proof of actual acquisition of appellants' communications is fatal to their

watchlisting claims.") Because a demonstration of standing is an "indispensable part of their case," and in order to prevail on their motion for summary judgment, Plaintiffs must support their allegations of standing "in the same way as any other matter on which [they] bear the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Bras v. Cal. Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan*, 504 U.S. at 561). Plaintiffs must proffer admissible evidence establishing both their standing as well as the merits of their claims. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) (holding that the court's ruling on summary judgment must be based only on admissible evidence); *see also Orr v. Bank of America NT & SA*, 285 F.3d 764, 773 (9 th Cir. 2001) (citing Fed. R. Evid. 901(a)) (holding that a trial court may only consider admissible evidence on ruling on a motion for summary judgment and authentication is a "condition precedent to admissibility"). If Plaintiffs are unable to make a showing sufficient to establish an essential element of their claim on which they bear the burden at trial, summary judgment must be granted against them. *See Celotex Corp.*, 477 U.S. at 322.

"To establish Article III Standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("*Clapper*") (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending." *Id.* (citing *Lujan*, 504 U.S. at 565 n.2) (emphasis in original). Thus, the Supreme Court has "repeatedly reiterated that 'the threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis in original)).

In order to establish standing on the remaining statutory grounds, Plaintiffs must be able to show that they have suffered an injury in fact that is (1) "concrete [and] particularized," (2) "fairly traceable to the challenged action[s]" of the defendants, and (3) "redressable by a

favorable ruling." *Clapper*, 568 U.S. at 409. In order to demonstrate that Plaintiffs have suffered the requisite injury in fact, Plaintiffs must, using publicly available facts, adduce admissible evidence that the contents of their communications or the metadata regarding those communications were subject to the intelligence-collection activities they challenge in this case. Plaintiffs must demonstrate that they "personally suffered a concrete and particularized injury in connection with the conduct about which [they] complain." *Trump v. Hawaii*, 138 S. Ct. 2392, 2416 (2018); *see also Clapper*, 568 U.S. at 411 ("[R]espondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory."); *Halkin*, 690 F.2d at 999-1000 (holding that the absence of proof of actual acquisition of appellants' communications was fatal to their claims).

In *Clapper*, the Court found that allegations that plaintiffs' communications would be intercepted were too speculative, attenuated, and indirect to establish injury in fact that was fairly traceable to the governmental surveillance activities. 568 U.S. at 408-13. The *Clapper* Court held that plaintiffs lacked standing to challenge the NSA's surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to establish a "certainly impending" injury. *Id.*

For their claim under the Wiretap Act, Plaintiffs must demonstrate an injury-in-fact occurred for each and every plaintiff where any communication traveling on the Internet backbone was intercepted, copied, or redirected, diverting it from its normal course. *See George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992), *cert. denied*, 506 U.S. 847 (1992)). For a claim under the Stored Communications Act, Plaintiffs must demonstrate an "injury from the collection, and maintenance in a government database, of records relating to them." *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (construing "intercept" in light of ordinary meaning, *i.e.*,, "to stop, or interrupt in progress or course before arrival.") (citation omitted).

///

///

C. Legal Standard on State Secrets Privilege.

The state secrets privilege has two applications: as a rule of evidentiary privilege, barring only the secret evidence from exposure during litigation, and as a rule of non-justiciability, when the subject matter of the lawsuit is itself a state secret, necessitating dismissal. *See Fazaga*, 916 F.3d at 1227; *see also American Civil Liberties Union v. National Security Agency*, 493 F.3d 644, 650 n.2 (6th Cir. 2007). The first application of evidentiary withholding can serve to remove only certain specific pieces of evidence or can be applied to compel the removal of a sufficiently broad swath of evidence which may have the consequence of requiring dismissal of the entire suit. Such a dismissal may be necessitated by the instances in which the removal of evidence disables a plaintiff from the ability to establish the *prima facie* elements of a claim without resort to privileged information or instances in which the removed evidence bars the defendant from establishing a defense. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

Once documents pursuant to a successful claim of privilege are withheld, the case may proceed with the omission of the secret or closely entangled evidence. Alternatively, if application of the state secrets bars too much, the court may be required to dismiss the action in its entirety. Such instances include when, without the secret evidence, a plaintiff is unable to prove the *prima facie* elements of a claim with nonprivileged evidence. *See id.* Or the privilege may apply to bar information that would otherwise give the defendant a valid defense to the claim, thus requiring dismissal. *See id.* Lastly, the court may be compelled to dismiss when, although the claims and defenses may be stated without reference to privileged evidence, "it may be impossible to proceed with the litigation because – privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses – litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2009) (en banc) (citations omitted); *see also Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 279-80 (4th Cir. 1980) (en banc) (per curiam) (Phillips, J., specially concurring and dissenting) (concluding that "litigation should be entirely foreclosed at the outset by dismissal of the

action" if it appears that "the danger of inadvertent compromise of the protected state secrets outweighs the public and private interests in attempting formally to resolve the dispute while honoring the privilege").

Alternatively, the state secrets privilege may be invoked to bar litigation of the matter in its entirety where "the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated." *Totten v. United States*, 92 U.S. 105, 107 (1875). Where the very subject matter of the lawsuit is a matter of state secret, the action must be dismissed without reaching the question of evidence. *See Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1197 (9th Cir. 2007) ("*Al-Haramain*") (citations omitted); *see also Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005) (holding that dismissal is proper where "sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters.").

D. Analysis of Plaintiffs' Standing.

The Court finds that two of the required elements for standing are at issue at this procedural posture: the question whether any individual plaintiff suffered any concrete and particularized injury as well as the issue whether any potential injury could possibly be found to be redressable by a favorable judgment. The Court addresses both elements in order.

1. Plaintiffs' Evidentiary Proffer of Their Alleged Injury.

Throughout the pendency of this action, Plaintiffs have consistently argued that they have suffered injury by the creation of a large, untargeted, dragnet surveillance program designed to "intercept all or substantially all of its customers' communications, . . . [which] necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using AT&T services." *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 1001 (N.D. Cal. 2006). In this matter, the Ninth Circuit has held that although the harm alleged by Plaintiffs is widely shared, that does not necessarily render it a generalized grievance. *See Jewel*, 673 F.3d at 909-10 ("[W]e

conclude that Jewel alleged a sufficiently concrete and particularized injury, Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches.").

However, at the summary judgment stage where their allegations must be supported by specific facts, Plaintiffs continue to maintain that the NSA's surveillance programs must have been comprehensive to be effective. Plaintiffs assert that their allegations regarding whether their communications were intercepted in mass surveillance efforts are more likely than not true because of the large, untargeted nature of the program. Precisely this argument was rejected by the court in *Obama v. Klayman*, in which the court found that the assertions of standing based on mass comprehensive surveillance were too speculative and ultimately unpersuasive. 800 F.3d at 567 (holding that plaintiffs' "assertion that NSA's collection must be comprehensive in order for the program to be most effective is no stronger than the *Clapper* plaintiffs' assertions regarding the government's motive and capacity to target their communications."). In the absence of a factual predicate to establish any particular harm on behalf of any specific individual plaintiff, the Court must review and adjudicate the effect of the classified evidence regarding Plaintiffs' standing to sue. That review and adjudication is contained in the Court's Classified Order filed herewith.

In their attempt to establish the specific factual predicate based on public evidence for their contention that Plaintiffs have, as specific named individuals, been injured by interception of their communications, Plaintiffs rely in large part on the declarations of Mark Klein and James W. Russell and their proffered experts, as well as an additional former AT&T employee to present the relevant operational details of the surveillance program. Just as they had before when contesting the violation of their Fourth Amendment rights, Plaintiffs assert that these declarations support the contention that customers' communications were the subject of a dragnet seizure and search program, controlled by or at the direction of the Defendants. Having reviewed the factual record in its entirety, the Court finds the Plaintiffs' evidence does not support this claim.

Plaintiffs again rely on the declaration of Klein, a former AT&T technician who executed a declaration in 2006 about his observations involving the creation of a secure room at

the AT&T facility at Folsom Street in San Francisco. (Dkt. No. 84-2, Declaration of Mark Klein ("Klein Decl.") ¶¶ 8-18.) However, the Court confirms its earlier finding that Klein cannot establish the content, function, or purpose of the secure room at the AT&T site based on his own independent knowledge. *See* Fed. R. Civ. P. 56(c)(4). The limited knowledge that Klein does possess firsthand does not support Plaintiffs' contention about the actual operation of the data collection process or the alleged agency role of AT&T. Klein can only speculate about what data were actually processed and by whom in the secure room and how and for what purpose, as he was never involved in its operation. Lastly, the documents attached to Klein's declaration are not excepted from the hearsay objection on the basis that they are admissible business records. (Dkt. No. 84-3, 84-4, 84-5, 84-6, Klein Decl. Exs. A-C.) The timing of the creation of these attachments indicate that they were not simultaneous records of acts or events that were occurring at or around the time of the documents' creation. *See* Fed. R. Evid. 803(6).

Plaintiffs again propound the declaration of James Russell who relies on the Klein declaration and attached exhibits with regard to the interconnections between AT&T and other internet providers. (Dkt. No. 84-1, Declaration of James W. Russell ¶¶ 5, 6, 10, 12, 19-22.) Having twice found those exhibits inadmissible for the truth of the matters asserted therein, the Court similarly finds Russell's proffered conclusions unreliable.

To this existing evidentiary record, Plaintiffs now add the declaration of another former technician at AT&T, Phillip Long, who declares that without explanation, "sometime in the first half of the 2000s," he was directed to reroute AT&T's Internet backbone connections through the Folsom Street facility, "rather than through the nearest frame relay or ATM switch." (Dkt. No. 417-5, Declaration of Phillip Long ¶¶ 11, 12.) Long declares that he can offer no engineering or business reason for this reconfiguration. (*Id*. at ¶ 15.) The addition of Long's declaration does not serve to corroborate AT&T's participation in the alleged governmental collection program.

Plaintiffs' previously-disclosed experts, J. Scott Marcus and Dr. Brian Reid, rely upon Klein's observations and documents to formulate their expert opinions. Just as the Court determined in the context of the Fourth Amendment cross-motions for summary judgment with

regard to the Marcus opinion, the Court finds that these expert conclusions are not based on sufficient facts or data where the underlying declaration is based on hearsay and speculation. For example, Dr. Reid, relying upon the description of the Folsom facility furnished by Klein, offers an opinion about the likelihood that Plaintiffs' communications "passed through the peering site at AT&T's Facility . . . along with the rest of the traffic passing over all of the peering-link fibers into which splitters were installed . . . were replicated." (Dkt. No. 417-6, Declaration of Brian Reid ¶¶ 2, 20-23.) As the Court has found, the evidence relied upon by Plaintiffs' experts regarding the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b).

In addition to these experts, Plaintiffs now proffer the opinions of two more experts, Ashkan Soltani and Matthew Blaze. Like the experts earlier proffered by Plaintiffs, Professor Blaze opines that, after review of the Klein declaration and exhibits, he believes "it is highly likely that the [internet] communications of all plaintiffs passed through peering-link fibers connected to the splitter . . . at the AT&T Folsom Street Facility." (Dkt. No. 417-7, Declaration of Matthew Blaze ¶¶ 2, 11, 41-46.) Again the Court has found that the evidence relied upon by Plaintiffs' expert regarding the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b). Lastly, Plaintiffs proffer Mr. Soltani as an expert who opines that a surveillance network of the type Plaintiffs conjecture would also likely intercept the communications of users of cloud-based email applications such as Google's gmail or Yahoo mail. (Dkt. No. 417-8, Declaration of Ashkan Soltani ¶ 16.) This unquantified likelihood of interception regarding some users' email based on the posited Internet surveillance connection points and collection process is insufficient to constitute specific evidence of injury. Further, the premise upon which Mr. Soltani's opinion derives is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b).

Plaintiffs further make the unsupported allegation that AT&T, Verizon, Verizon Wireless, and Sprint were acting in concert with or as agents of Defendants to produce phone

records in bulk.[1] Plaintiffs contend that the Government has admitted that these large service providers were participants in the NSA bulk collection of telephony metadata. In support of this contention, Plaintiffs submit a Primary Order issued by the Foreign Intelligence Surveillance Court ("FISC") authorizing the NSA to collect such bulk data for a 90-day period, from unidentified, redacted telecommunications service providers. (Dkt. No. 417-4, Declaration of Richard R. Weibe, Ex. A at 1.) This redacted order was issued in FISC docket Business Records ("BR") 10-10 and was declassified and publicly released by the Director of National Intelligence. (*Id.* at ¶ 3.) Plaintiffs also offer a copy of an excerpt from an NSA Inspector General compliance audit report which includes a letter regarding a non-compliance incident in the telephone call records program. (*See id.*, Ex. B at 28-29.) The excerpt of the report and attached letter were released in response to a Freedom of Information Act ("FOIA") lawsuit brought by the New York Times against the National Security Administration in 2015. (*See id.* at ¶ 4.) The letter, filed with the FISC, identifies in the caption the telecommunications companies, including AT&T, Verizon, Verizon Wireless, and Sprint, that were compelled by the Primary Order BR 10-10 to produce records. (*Id.*, Ex. B at 28.)

In response, Defendants contend that, although the redacted Primary Order from the FISC (in which the names of the providers were redacted) was authenticated by the Government, the second letter (which purports to identify the names of those providers) has not been authenticated by the Government.[2] Because the letter was inadvertently disclosed in an

---

[1] Plaintiffs have only been able to establish that the Government has admitted to working with Verizon Business Network Systems for a brief period of time, which does not indicate that data from other network providers were ever collected. *See Obama*, 800 F.3d at 563 (holding that because "plaintiffs are Verizon *Wirelesss* subscribers and not Verizon *Business Network Systems* subscribers . . . the facts marshaled by plaintiff do not fully establish that their own metadata was ever collected.").

[2] Defendants also argue that the letter has no evidentiary value as it was downloaded by Plaintiffs from the New York Times article written about the FOIA lawsuit. *See Schwarz v. Lassen County ex rel. Lassen County Jail*, 2013 WL 5425102, at *10 (E.D. Cal. Sept. 27, 2013) ("evidence procured off the Internet is adequate for almost nothing" without authentication). However, in response, Plaintiffs proffer the affidavit of an attorney for the New York Times in the FOIA lawsuit, who declares that the excerpt and attached letter were produced by the NSA in August 2015 in that matter. (*See* Dkt. No. 431, Declaration of David E. McGraw, ¶¶ 2, 5-6.) Mr. McGraw indicates that the attorneys representing the NSA at the Department of Justice notified him that the letter contained in the audit report had been "inadvertently produced" and had asked for its return. (*Id.* at ¶ 7.)

unrelated matter and has not been authenticated by the Government, the Court finds it cannot rely on it. *See, e.g., Al-Haramain*, 507 F.3d at 1205. Further, there has been no waiver of the state secret privilege over the document. The Court accepts Defendants' representation that whether or not the letter is authentic is itself classified information the disclosure of which could reasonably be expected to cause grave harm to national security. (*See also* Dkt. No. 422, Notice of Lodging of Classified Materials for *In Camera, Ex Parte* Review at 2, Declaration of Jonathan Darby, National Security Agency Director of Operations, ¶¶ 16-20.)

Lastly, Plaintiffs seek to introduce what is labeled a working draft of a report prepared by the Office of the Inspector General for the National Security Agency ("Draft OIG Report") with a supporting declaration from Edward Snowden. (Dkt. No. 432, Declaration of Edward J. Snowden, Ex. 1; Dkt. No. 147, Declaration of Richard R. Wiebe, Ex. A.) The Draft OIG Report does not in fact name AT&T or Verizon as participants in any possible collection efforts, it is labeled as a draft, and Defendants do not authenticate the exhibit. Accordingly, the Court finds it cannot rely on it. *See, e.g., Al-Haramain*, 507 F.3d at 1205. Plaintiffs' contention that Snowden may authenticate the purported NSA document is not persuasive, either by way of his current declaration or in the future through live testimony. *See Orr*, 285 F.3d at 773 (holding that a trial court may only consider admissible evidence on ruling on a motion for summary judgment and authentication is a "condition precedent to admissibility"). Further, there has been no waiver of the state secret privilege over the document and Defendants have objected on the basis of the privilege to Plaintiffs' requests for admissions regarding the authenticity of this document. (Dkt. No. 414-1, Government Defendants' Supplemental and Revised Response to Plaintiffs' Revised First Set of Requests for Admission Limited to Standing, at 70-73.)

The underlying premise that AT&T worked in the capacity of an agent for Defendants is without factual or substantive evidentiary support. And Plaintiffs have still not adduced admissible evidence of the actual equipment installed in the secure room or the activities conducted there. After review of the entirety of the evidentiary record, the Court finds the propounded evidence is not probative or admissible as to the actual conditions or purposes of the apparatus at the AT&T facility or their role at the time at issue in this case.

The Court finds that Plaintiffs have failed to proffer sufficient admissible evidence to indicate that records of their communications were among those affected by Defendants. Although there are materials in the public record that allude to possible surveillance programs, the Court finds that the "argument that 'the cat is already out of the bag' is unsupported by the record and contrary to the government's" classified submissions. *See Military Audit Project v. Casey*, 656 F.2d 724, 744-45 (D.C. Cir. 1981). Although in this public order, the Court is unable to address the sum of all evidence relevant to standing, the Court has addressed the classified evidence relating to standing in detail in its Classified Order, filed in conjunction with this one. (*See* Classified Order Section I.) Although neither the Court nor Defendants can confirm or deny the allegations as made by Plaintiffs in their proffer of evidence in support of standing, the Court addresses the operative, but classified, facts separately in detail.

In addition, having reviewed the classified portion of the record, the Court concludes that even if the public evidence proffered by Plaintiffs were sufficiently probative to establish standing, adjudication of the standing issue could not proceed without risking exceptionally grave damage to national security. The details of the alleged data collection process that are subject to the Defendants' assertion of the state secrets privilege are necessary to address Plaintiffs' theory of standing as well as to engage in a full and fair adjudication of Defendants' substantive defenses.

2. Redressability.

Another necessary element to establish Article III standing is the requirement that any concrete and particularized injury be "redressable by a favorable ruling.'" *Clapper*, 568 U.S. at 409. Here, the Court cannot issue a judgment without exposing classified information. And, by evaluating the classified information, the Court has determined that it cannot render a judgment either as to the merits or as to any defense on the issue of standing. Any finding or final judgment would disclose information that might imperil the national security. *See, e.g., Klayman*, 800 F.3d at 568 (finding that "the government's silence regarding the scope of bulk collection is a feature of the program, not a bug.") (citing *Clapper*, 568 U.S. at 412 n.4 ("the court's postdisclosure decision about whether to dismiss the suit for lack of standing would

surely signal to the terrorist whether his name was on the list of surveillance targets.")). The same "considerations apply with equal force here, where the government has sought to maintain a similarly strategic silence regarding the scope of its bulk collection." *Id.* In order to issue a dispositive decision on the standing issue, a finding of standing would necessitate disclosure of possible interception of plaintiffs' communications, thereby signaling injury. Such a disclosure may imperil national security. Any attempt to prove the specific facts of the programs at issue, or to defend against the Plaintiffs' analysis of the programs would risk disclosure of the locations, sources, methods, assisting providers, and other operational details of Defendants' intelligence-gathering activities. At this advanced procedural posture, the Court is bound to accept the Defendants' representation that disclosure of these details reasonably could be expected to cause exceptionally grave damage to national security.

Even if, utilizing only public evidence, the Plaintiffs could ostensibly plead sufficient facts to support their claim of standing to pursue their remaining statutory causes of action, the Court finds that it faces the intractable problem that proceeding further with this case would cause exceptionally grave harm to the national security. The Court cannot issue any determinative finding on the issue of whether or not Plaintiffs have standing without taking the risk that such a ruling may result in potentially devastating national security consequences. *See, e.g., Clapper*, 568 U.S. at 412 n.4. Notwithstanding the fact that this Court has thoroughly reviewed all of the evidence submitted with regard to Plaintiffs' standing, making any determination to address Plaintiffs' allegations regarding the scope of the data collection program would risk informing adversaries of the specific nature and operational details of the process and scope of Defendants' participation in the program. Accordingly, the Court finds that Plaintiffs are unable to show either that they have suffered a concrete and particularized injury or that any such potential injury could be redressable by a favorable ruling. As the Ninth Circuit predicted early on in the development of this case, "procedural, evidentiary, and substantive barriers" might ultimately doom Plaintiffs' proof of standing. *Jewel*, 673 F.3d at 911. This Court found, and the Ninth Circuit has affirmed, that the assertion of the state secrets privilege did not warrant dismissal at the pleadings stage without a thorough and complete

investigation of the evidence. *Jewel*, 965 F. Supp. 2d 1090, 1105-06 (N.D. Cal. 2013); *Jewel*, 673 F.3d at 909-10; *see also Fazaga*, 916 F.3d at 1226, 1232, 1234. However, the Court, after extensive *in camera* review of the classified materials and a similarly thorough review of the public evidence, finds that making any particularized determination on standing in order to continue with this litigation may imperil the national security.[3] The Court also addresses this finding in its Classified Order.

E. Defendants' Assertion of the State Secrets Privilege.

The privilege asserted by Defendants here seeks to protect information vital to the national security and may be invoked by the Government where it is shown, "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 6-7 (1953).

The analysis of whether the state secrets privilege applies involves three distinct steps. First, the Court must ascertain whether the procedural requirements for invoking the privilege have been satisfied. *Jeppesen*, 614 F.3d at 1080 (quoting *Al-Haramain*, 507 F.3d at 1202). Second, the Court must make an independent determination whether the information is privileged. In determining whether the privilege attaches, the Court may consider a party's need for access to the allegedly privileged materials. *See Reynolds*, 345 U.S. at 11. Lastly, the "ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim." *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007).

In order to satisfy the requirements of the first step, the Government must submit a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* (quoting *Reynolds*, 345 U.S. at 7-8). The assertion of privilege "must by presented in sufficient detail for the court to make an

[3] After thorough review of the evidence submitted in relation to Plaintiffs' statutory claims and marshaled by Defendants to satisfy the Court's broader order regarding the threshold standing issue, the Court is satisfied that its analysis of the Fourth Amendment standing to sue remains law of the case and rests on solid legal ground. *See Jewel v. National Security Agency*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015). Therefore, Plaintiffs' request to reconsider that decision is DENIED.

independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Id.* Such an invocation must be made only after "serious, considered judgment, not simply [as] an administrative formality." *United States v. W.R. Grace*, 526 F.3d 499, 507-08 (9th Cir. 2008) (en banc). "The formal claim must reflect the certifying official's personal judgment . . . [and] must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Jeppesen*, 614 F.3d at 1080.

The Court finds that this step has been satisfied by the submission of the public declaration of the Principal Deputy Director of National Intelligence, serving as Acting Director of National Intelligence and acting head of the Intelligence Community, following her personal consideration of the matters at issue here. (*See* Dkt. No. 388-2, Declaration of Principal Deputy Director of National Intelligence, ¶¶ 8, 19; Dkt. No. 104, Declaration of James R. Clapper ¶ 2; Dkt. No. 168, Declaration of James R. Clapper ¶ 2.) This claim of privilege is further supported by the declaration of Admiral Michael Rogers, in which he explains the nature of the evidence itself and details the specific harms that could be expected to result from disclosure of the information. (*See* Dkt. No. 389, Rogers Decl. ¶¶ 2, 331; *see also* Classified Order at n.1.)

In order to satisfy the requirements of the second step, the Court is able to assess independently, based on both the public and classified submissions by Defendants, and from all of the evidence in the record accumulated over the years of litigating this case, that there is a reasonable danger the disclosure of the information at issue here would be harmful to national security. *See, e.g., Jewel*, 965 F. Supp. 2d at 1103; *Jewel*, 2015 WL 545925, at *1, *5. The Court must "sustain a claim of privilege when it is satisfied, 'from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged.'" *Jeppesen*, 614 F.3d at 1081 (quoting *Reynolds*, 345 U.S. at 10). Here, the Court has made "an independent determination whether the information is privileged." *Al-Haramain*, 507 F.3d at 1202. In making this determination, the Court must strike the appropriate balance "between protecting national security matters and preserving an open court system." *Id.* at 1203. "This inquiry is a difficult

one, for it pits the judiciary's search for truth against the Executive's duty to maintain the nation's security." *El-Masri*, 479 F.3d at 304. In evaluating the need for secrecy, the Court must defer to the Executive on matters of foreign policy and national security. *See Jeppesen*, 614 F.3d at 1081-82. However, the assertion of the state secrets doctrine does not "represent a complete surrender of judicial control over access to the courts." *El-Masri*, 479 F.3d at 312. Rather, in order to ensure that the doctrine is not asserted more frequently and sweepingly than necessary, "it is essential that the courts continue critically to examine instances of its invocation." *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983). However, should the Court find that the materials must not be divulged, "the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it." *See Jeppesen*, 614 F.3d at 1081 (citing *Reynolds*, 345 U.S. at 11).

The final element of the determination regarding the Government's assertion of the state secrets privilege is the court answering the ultimate question regarding how the matter should proceed in light of the legitimate claim of privilege. *See Jeppesen*, 614 F.3d at 1080. "The court must assess whether it is feasible for the litigation to proceed without the protected evidence and, if so, how." *Id.* at 1082. When the Government successfully invokes the state secrets privilege, "the evidence is completely removed from the case." *Kasza*, 133 F.3d at 1166. The court is then tasked with disentangling the nonsensitive information from the privileged evidence. Often, after the privileged evidence is excluded, "the case will proceed accordingly, with no consequences save those resulting from the loss of evidence." *Al-Haramain*, 507 F.3d at 1204 (quoting *Ellsberg*, 709 F.3d at 64). However, there "will be occasions when, as a practical matter, secret and nonsecret information cannot be separated. In some cases, therefore, 'it is appropriate that the courts restrict the parties' access not only to evidence which itself risks the disclosure of a state secret, but also those pieces of evidence or areas of questioning which press so closely upon highly sensitive material that they create a high risk of inadvertent or indirect disclosures.'" *Jeppesen*, 614 F.3d at 1082 (quoting *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1143-44 (5th Cir. 1992)); *see also Kasza*, 133 F.3d at 1166 ("[I]f seemingly innocuous information is part of a . . . mosaic, the state secrets privilege

may be invoked to bar its disclosure and the court cannot order the government to disentangle this information from other [*i.e.*, secret] information.")

Plaintiffs maintain that the Ninth Circuit's recent decision in *Fazaga* precludes the Court from dismissing this case on state secrets grounds, and that the Court must use the procedures of Section 1806(f) to decide Plaintiffs' statutory claims notwithstanding Defendants' assertions that even a finding on the threshold question of standing will cause grave harm to national security. *Fazaga* addressed a challenge to an allegedly unlawful FBI counter-terrorism investigation involving electronic surveillance. 916 F.3d at 1210-11. The district court dismissed all but one of plaintiff's claims at the pleading stage without further discovery based on the Government's assertion of the state secrets privilege. *Id.* at 1211. The Ninth Circuit reversed, concluding that Section 1806(f)'s procedures are to be used when "aggrieved persons" challenge the legality of electronic surveillance and that the district court erred by dismissing the case without reviewing the evidence, "including the evidence over which the Attorney General asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted." *Id.* at 1238, 1252.

Defendants contend that the *ex parte*, *in camera* procedures authorized under Section 1806(f) apply only to the determination of whether alleged electronic surveillance was lawful, and not to the threshold determination of whether Plaintiffs are "aggrieved persons" who have been subject to surveillance in the first place. *See, e.g.*, *Wikimedia Foundation v. National Security Agency*, 335 F. Supp. 3d 772, 786 (D. Md. 2018). In other words, in Defendants' view, Section 1806(f) displaces the state secrets privilege only as to a determination of lawfulness *after* Plaintiffs' standing has been demonstrated using non-classified evidence. The Court notes that in the procedural posture in which *Fazaga* reached the Ninth Circuit, the plaintiff's status as an aggrieved person had not yet been tested through discovery. Thus, the Ninth Circuit was not presented with the issue of what to do when, as here, the answer to the question of whether a particular plaintiff was subjected to surveillance – *i.e.*, is an "aggrieved person" under Section 1806(f) – is the very information over which the Government seeks to assert the state secrets privilege. Instead, in remanding for further proceedings, the court in *Fazaga* held that "[t]he

complaint's allegations are sufficient *if proven* to establish that Plaintiffs are 'aggrieved persons.'" *Id.* at 1216 (emphasis added).

This Court owes significant deference to the Executive's determination that, as described at oral argument, even a simple "yea or nay" as to whether Plaintiffs have standing to proceed on their statutory claims would do grave harm to national security. *See Jeppesen*, 614 F.3d at 1081-82 ("In evaluating the need for secrecy, 'we acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena.'") (quoting *Al-Haramain*, 507 F.3d at 1203); *see also Al-Haramain*, 507 F.3d at 1203 ("[A]t some level, the question whether Al-Haramain has been subject to NSA surveillance may seem, without more, somewhat innocuous . . . . But our judicial intuition about this proposition is no substitute for documented risks and threats posed by the potential disclosure of national security information."). The Court has not "accept[ed] at face value the government's claim or justification of privilege" on the issue of Plaintiffs' standing to pursue their remaining statutory claims, but instead has reviewed all of the classified evidence submitted by Defendants in response to Plaintiffs' discovery requests and this Court's orders. *See id.* That comprehensive review distinguishes this case from *Fazaga*, and in fact from any other case involving state secrets cited by the parties or known to this Court. Under the unique procedural posture of this case, and where the very issue of standing implicates state secrets, the Court finds that it is not foreclosed under the holding in *Fazaga* and Section 1806(f) from now dismissing on state secrets grounds.

Here, having reviewed the materials submitted and having considered the claims alleged and the record as a whole, the Court finds that, just as they did when disputing the violation of the Fourth Amendment in the parties' previous cross-motions for summary judgment, Defendants have again successfully invoked the state secrets privilege. This Court has previously found and maintains that, given the multiple public disclosures of information regarding the surveillance program, the very subject matter of the suit does not constitute a state secret. However, at this procedural posture and with the development of a full and extensive

record on the threshold issue of standing, the Court finds that permitting further proceedings would jeopardize the national security.

The Court finds that because a fair and full adjudication of the Plaintiffs' claims and the Defendants' defenses would require potentially harmful disclosures of national security information that are protected by the state secrets privilege, the Court must exclude such evidence from the case. *See Jeppesen*, 614 F.3d at 1083 (holding that "application of the privilege may require dismissal" of a claim if, for example, "the privilege deprives the plaintiff of information needed to set forth a prima facie case, or the defendant of information that would otherwise give the defendant a valid defense to the claim"). Addressing any defenses involves a significant risk of potentially harmful effects any disclosures could have on national security. *See Kasza*, 133 F.3d at 1166.

Having allowed the full development of the record and having reviewed the universe of documents and declarations produced by both parties to this action both publicly and under the procedures of Section 1806(f) of FISA, the Court finds that it has reached the threshold at which it can go no further. The Court accepts the assertion of the state secrets privilege at this procedural juncture to mandate the dismissal of this action. Accordingly, based on both the determination that it cannot rule whether or not Plaintiffs have standing to proceed and that the well-founded assertion of privilege mandates dismissal, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion to proceed to resolution on the merits.[4]

F. Plaintiffs' Request for Additional Discovery and for Discovery Sanctions.

Further, having reviewed the universe of classified and public documents produced by Defendants, the Court is satisfied that Defendants have met their discovery obligations. (*See* Classified Order at 2.) The Court finds that no evidentiary sanction for evidence spoliation

[4] As to all remaining claims, judgment is entered against Government officials in their personal capacities for both damages and equitable relief under the Constitutional and statutory provisions. The personal-capacity claims were stayed pending "resolution of any dispositive motion by the Government Defendants." (Order granting stipulation, Dkt. No. 93 at 1-2.) Having granted summary judgment in favor of Defendants, all personal-capacity claims are resolved in Defendants' favor as well.

is warranted and there is no basis to grant Plaintiffs' request to continue the resolution of the cross-motions for summary judgment pursuant to Federal Rule of Civil Procedure 56(d). In light of the Court's determination that this action cannot proceed further, under Section 1806(f) or otherwise, disclosure to the Plaintiffs of the classified evidence submitted by Defendants is not "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Accordingly, Plaintiffs' renewed requests for access to the classified evidence Defendants have submitted, for a further declassification review of that evidence, and for further discovery or evidentiary sanctions are DENIED.

CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion for summary judgment. The Court shall issue a separate classified order which shall be preserved in the Court's sealed record pending any further proceeding. All classified evidence lodged with the Court by Defendants shall also be so preserved in the sealed record. A separate judgment will issue and the Clerk shall close the file.

IT IS SO ORDERED.

Dated: April 25, 2019

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE